UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BANCO DEL AUSTRO, S.A.	:	
Plaintiff,	:	Case No. 1:16-cv-00628 (LAK)
v.	:	
WELLS FARGO BANK, N.A.	:	
Defendant.	:	

DEFENDANT WELLS FARGO BANK, N.A.'S REPLY MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS THE COMPLAINT PURSUANT TO FRCP 12(b)(6)

Jeffrey J. Chapman
Aaron F. Jaroff
jchapman@mcguirewoods.com
ajaroff@mcguirewoods.com
McGuireWoods LLP
1345 Avenue of the Americas, 7th Floor
New York, New York 10105
(212) 548-2100

Attorneys for Defendant Wells Fargo Bank, N.A.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Defendant Wells Fargo[1] respectfully submits this reply memorandum in further support of its Motion to Dismiss the Complaint.

PRELIMINARY STATEMENT

This is a simple case governed by the framework of Article 4-A of the N.Y. U.C.C., which allocates the risk of loss between banks involved in wire transfers. In its Memorandum of Law in Opposition (the "Opposition Brief"), BDA raises a variety of inapplicable issues designed to distract from the only relevant matters: (i) BDA and Wells Fargo agreed that SWIFT authentication was a commercially reasonable security procedure for verifying SWIFT payment orders; (ii) BDA concedes that Wells Fargo complied with this security procedure; (iii) BDA did not provide Wells Fargo with instructions restricting the acceptance of SWIFT payment orders; and (iv) BDA has not alleged that Wells Fargo acted in bad faith.

BDA spends much of the Opposition Brief discussing whether Wells Fargo behaved as a prudent bank and followed the USA PATRIOT Act, the Bank Secrecy Act ("BSA"), and other anti-money laundering ("AML") and "Know Your Customer" ("KYC") statutes and regulations. BDA speculates that these rules required Wells Fargo to conduct due diligence for BDA's benefit and to stop the transfers at issue. But compliance with these statutes and regulations is irrelevant to Wells Fargo's obligations under the N.Y. U.C.C., the Agreement, and common law. Any obligations these rules impose were not part of the Agreement's security procedures for verifying the authenticity of BDA's SWIFT payment orders. Nothing about BDA's distinguishable authority from outside of the Second Circuit suggests otherwise. BDA would have this Court impose liability on Wells Fargo for processing payment orders that were

[1] Unless otherwise noted, capitalized terms are as defined in Wells Fargo's Memorandum of Law in Support of its Motion to Dismiss (the "Opening Brief"). ECF No. 15. All references to "Ex. [_]" are to the exhibits of the Declaration of Jeffrey J. Chapman, filed on February 18, 2016. ECF No. 14.

authorized and verified pursuant the parties' Agreement. To do so would subject every financial institution processing payment requests to endless second guessing – essentially requiring that they contact their customers multiple times whenever a payment order is received. This is not what was intended by the N.Y. U.C.C.'s risk transfer provisions, and it would eviscerate the efficiencies that wire transfers and SWIFT payment orders were designed to promote. The Court should decline to impose such a burdensome and impractical regime.

ARGUMENT

I. Wells Fargo Fulfilled Its Obligations Under the N.Y. U.C.C.

BDA cannot overcome Wells Fargo's showing that the Unauthorized Transfers were "effective" as BDA's order pursuant to Section 4-A-202(2), precluding liability for its losses.[2]

A. BDA Agreed SWIFT Authentication Was Commercially Reasonable.

Relying on secondary authority and a First Circuit decision, BDA attempts to effectively nullify its Agreement with Wells Fargo, ignoring the fact that *it agreed* that "[f]or SWIFT, the SWIFT Authentication procedures in accordance with the SWIFT User Handbook" was a "commercially reasonable" security procedure. Compl. Ex. A ¶ 3.1. BDA implies that the Agreement is somehow not applicable because Wells Fargo applied an inappropriate "one-size-fits-all" approach to its security procedure for SWIFT payment orders. Opposition Brief at 12. This is simply untrue, as BDA also *agreed* that verifying SWIFT messages[3] via SWIFT Authentication procedures was "commercially reasonable in light of [BDA's] *circumstances* and

---

[2] BDA states that the transfers at issue were not authorized pursuant to Section 4-A-202(1) because they were initiated by an unauthorized user who "remotely accessed BDA's computer system." Opposition Brief at 9-10. At this stage, Wells Fargo does not dispute that the transactions at issue were unauthorized based on the Complaint's allegations, and any analysis under Section 4-A-202(1) is irrelevant.

[3] There is no dispute that SWIFT is one of the most prevalent ways to send payment orders. *See* INTRODUCTION TO SWIFT, https://www.swift.com/about-us/discover-swift (last visited Apr. 22, 2016) (noting SWIFT is used by over 11,000 organizations across the world).

the *type*, *value* and *frequency* of the payment orders [BDA] will request." Compl. Ex. A ¶ 3.1 (emphasis added). It was not one-size-fits-all, as BDA agreed. The sole case that BDA cites in support of its position is distinguishable, as it examined "internet banking – also known as 'eBanking,'" not payment orders sent via a network like SWIFT.[4] *See Patco Constr. Co., Inc. v. People's United Bank*, 684 F.3d 197, 200 (1st Cir. 2012). As BDA admitted, the Unauthorized Transfers were sent via the SWIFT network from its own SWIFT terminal. Compl. ¶¶ 20, 31. Therefore, the only applicable security procedures are those for SWIFT payment orders, which BDA and Wells Fargo agreed would be "the SWIFT Authentication procedures in accordance with the SWIFT User Handbook." Compl. Ex. A ¶ 3.1. BDA cannot now revise the Agreement because of the unfortunate breach of its systems.[5] *See* N.Y. U.C.C. § 4-A-203 cmt. 4 (explaining that Section 4-A-202 does not make banks "insurers against fraud" and that a security procedure "is not commercially unreasonable simply because another procedure might have been better").

B. BDA Admits Wells Fargo Complied with the Security Procedure.

BDA does not dispute that Wells Fargo verified the payment orders at issue using SWIFT authentication. Instead, it argues that Wells Fargo failed to adhere to the provision of 4-A-202(2) that requires a receiving bank to also comply with "any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer." N.Y. U.C.C. § 4-A-202(2); *see* Opposition Brief at 15-16, 21-22. However, BDA has cited

---

[4] The sole authority that BDA cites regarding SWIFT, a journal article from 2002, notes only that SWIFT "may" be vulnerable to hacking. Opposition Brief at 12. If BDA had any concerns with the commercial reasonableness or security of the SWIFT network it could have – and should have – raised them when entering into the Agreement with Wells Fargo in 2011.

[5] BDA notes that Section 4-A-203 of the N.Y. U.C.C. is "not at issue." Opposition Brief at 9 n.9. Section 4-A-203 provides customers with a potential defense once a receiving bank demonstrates that the relevant transfers were effective as the orders of the customer under Section 4-A-202(2). *See* Opening Brief at 15-17. As BDA admits that Section 4-A-203 does not apply, and alleges that the payment orders resulted from the theft of its own employee information, Wells Fargo is entitled to the full dismissal of BDA's statutory claim. *See id.*

nothing to suggest that it provided Wells Fargo with *any agreement or instruction restricting acceptance* of SWIFT payment orders. If BDA wanted Wells Fargo only to accept payment orders during certain times or sent to certain places, or to reject those that were deemed unusual by Wells Fargo's separate AML-related monitoring, it could have negotiated for those restrictions in the Agreement's security procedure for SWIFT payment orders. *See generally* N.Y. U.C.C. § 4-A-203 cmt. 3. It chose not to do so.[6]

The security procedure governing SWIFT payment orders is clearly defined on page 4, Paragraph 3.1 of the Agreement. Compl. Ex. A ¶ 3.1. Despite the absence of any restrictions in the SWIFT security procedure beyond verification using SWIFT authentication, BDA now belatedly attempts to include further procedures that it argues are based on the KYC and due diligence requirements flowing from the USA PATRIOT Act, the BSA, and other AML and sanction-related statutes and regulations. Opposition Brief at 15-22. BDA even speculates that, because Wells Fargo demonstrated in the Opening Brief that it satisfied its obligations under the Agreement and the N.Y. U.C.C. by confirming that the SWIFT payment orders originated from BDA pursuant to the agreed-upon security procedure, it did not have *any* transaction monitoring systems or other AML-related safeguards. BDA is of course wrong. Wells Fargo has these systems, spends millions of dollars ensuring that they are functioning and compliant, and is examined by multiple regulators to determine that such systems are sufficient. However, these complex and varied procedures are irrelevant, as (i) they were not part of the Agreement's security procedure for verifying SWIFT payment orders and (ii) they were not designed to protect customers such as BDA from undetected breaches of their security systems.

---

[6] As a result, BDA's argument that the preclusive effect of Article 4-A of the N.Y. U.C.C. is somehow limited because the parties agreed to restrict the acceptance of payment orders, Opposition Brief at 33 n.21, fails as well. *See infra* Section III.

Wells Fargo does not dispute that the Agreement notes that it is governed by "the Laws of the US and the State of New York, including (without limitation) Articles 3, 4, 4A, and 5 of the Uniform Commercial Code" or that it informed BDA that it "intend[ed] to comply with all Laws of the US applicable to it, including without limitation the USA PATRIOT Act" and AML and other sanction-related regulations. Compl. Ex. A ¶¶ 7.7-7.8. However, the Agreement's general reference to compliance with such statutes and regulations was not incorporated into, or made a part of, the security procedures that BDA agreed would govern SWIFT payment orders, nor did it serve as an agreement or instruction to restrict the acceptance of payment orders issued in the name of BDA.[7] The parties specifically addressed how SWIFT payment orders would be verified in Paragraph 3.1 of the Agreement, and New York "follows the common (and commonsensical) rule [of contractual interpretation] that a specific provision . . . governs the circumstance to which it is directed, even in the face of a more general provision." *Capital Ventures Int'l v. Republic of Argentina*, 652 F.3d 266, 271 (2d Cir. 2011).

Finally, BDA does not dispute the well-settled authority stating that the due diligence contemplated by these statutes was designed to ensure that banks could detect and prevent the potential money-laundering activity of their own customers, not to protect their customers from the hacking of their own computer systems, rendering such statutes further inapplicable to BDA's claims. *See Silverman Partners, L.P. v. First Bank*, 687 F. Supp. 2d 269, 282 (E.D.N.Y. 2010) (such statutes were "intended to protect the banks and the general public from harm," not establish a standard of care); *see also infra* Section II.B; Opening Brief at 17-18.

---

[7] The same is true for the July 14, 2014 letter describing Wells Fargo's Global Financial Crimes Risk Management Program, attached as Exhibit 2 to the Opposition Brief (the "FCRM Letter"). The FCRM Letter simply explains Wells Fargo's compliance with the BSA, AML and counter-terrorism financing regulations, and sanctions imposed by the Office of Foreign Assets Control. FCRM Letter at 1. Nothing in the FCRM Letter can be considered a written agreement or instruction of BDA restricting acceptance of payment orders.

C. Wells Fargo Accepted the Payment Orders in Good Faith.

BDA fails to address the binding Second Circuit precedent cited in the Opening Brief, which holds as a matter of law that BDA must plead and prove bad faith or willful misconduct. *See* Opening Brief at 12-15. BDA relies solely on a lower court decision from Michigan, and tries to argue that Wells Fargo did not accept the payment orders at issue in good faith because it chose to ignore "red flags" presumably similar to those in *Experi-Metal, Inc. v. Comerica Bank*, No. 09-cv-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011). *See* Opposition Brief at 22-24. *Experi-Metal*, which involved a car parts manufacturer, not a sophisticated banking entity such as BDA, is not persuasive in light of Second Circuit authority and is factually distinguishable. The wrongdoers in *Experi-Metal* perpetrated their fraud by logging directly into the defendant bank's system – over which the bank undoubtedly had responsibility for monitoring – rather than here, where the unauthorized users accessed BDA's SWIFT terminal through BDA's internal systems. *See Experi-Metal*, 2011 WL 2433383, at *7; *see also* Compl. ¶¶ 20, 31. Further, the *ninety-three* fraudulent payment orders in *Experi-Metal* were sent over a period of just *seven hours* to banks "in destinations where most cyber-crime has been traced (i.e. Russia and Estonia)." *Experi-Metal*, 2011 WL 2433383, at *7. This is a far cry from twelve payment orders sent over a ten-day period to the banking and commercial centers of Hong Kong, New York, Dubai, and Los Angeles.[8] Compl. ¶ 23. Finally, the fraudulent transfers in *Experi-Metal* resulted in the complete emptying of one account at issue and a $5 million overdraft in another, facts which are absent from BDA's allegations. *Experi-Metal*, 2011 WL 2433383, at *7.

BDA suggests that Wells Fargo did not act in good faith because it failed to apply its

[8] BDA repeatedly argues that Wells Fargo should have been alerted to the fraudulent nature of the payment orders because some beneficiaries were located in the "reputed money laundering hub" of Hong Kong. Opposition Brief at 5, 6, 23, 29. This ignores that Hong Kong is also a major international financial center to which thousands, if not hundreds of thousands, of wire transfers and payment orders are sent each day in the normal course of business.

policies designed to detect unusual activity to block or reject the payment orders. Opposition Brief at 22-24. However, unlike *Experi-Metal*, there was nothing "unusual" about these orders, *see* Opening Brief at 14-15, and such policies were not designed to protect BDA or reject or block authorized, authenticated payment orders. *See supra* Section I.B; Opening Brief at 17-18. BDA has not pointed to a single case suggesting that the use of SWIFT authentication to verify SWIFT payment orders represents a failure to accept the orders in good faith. At most, allegations that Wells Fargo should have "employed more advanced fraud detection" suggests negligence, not a lack of "honesty in fact or a failure to observe reasonable commercial standards of fair dealing," or bad faith, as the Court of Appeals has held. *See J. Walter Thompson, U.S.A., Inc. v. First BankAmericano*, 518 F.3d 128, 139-40 (2d Cir. 2008) (quotation omitted).

II. BDA Fails to Allege a Claim for Negligence.

A. BDA Misstates the Agreement, Which Prohibits Negligence Claims.

BDA is incorrect when it states that Paragraph 2.3 of the Agreement permits its negligence claim. Opposition Brief at 29 n.19, 34. When quoting the Agreement, BDA omits precisely the language that, with Paragraph 7.15, prohibits any claims for negligence. *See* Opening Brief at 22-24. The full text from the Agreement states:

> Subject to the next sentence, if [BDA] is able to show that Wells Fargo failed to exercise ordinary care in paying any unauthorized transaction and that Wells Fargo's failure directly and substantially contributed to a loss, the parties agree that the loss will be allocated between Wells Fargo and [BDA] based on the extent to which Wells Fargo's failure to exercise ordinary care contributed to the loss. [BDA] agrees that Wells Fargo does not fail to exercise ordinary care . . . (ii) because Items are forged[,] counterfeited, or altered in such a manner that a reasonable person would not detect such forgery, counterfeit, or alteration.

Compl. Ex. A ¶ 2.3 (omitted text underlined). BDA admits that the payment orders at issue were altered by an unauthorized user such that they were indistinguishable from validly authorized orders. *See* Ex. 4 at 3 (stating that an unauthorized user "altered the amounts, the beneficiary,

and the destination" for the Unauthorized Transfers); Compl. ¶¶ 20, 31. It is therefore undeniable that the payment orders were "altered in such a manner that a reasonable person would not detect" the alteration. Compl. Ex. A ¶ 2.3. Indeed, BDA did not detect the alterations until well after the payment orders were sent. In such circumstances BDA agreed that Wells Fargo specifically *did not* fail to exercise ordinary care, thus prohibiting its negligence claim. *Id.*

B. Wells Fargo Did Not Breach Any Duty Owed to BDA.

Notwithstanding the fact that its negligence claim is specifically addressed and prohibited by the Agreement, BDA attempts to bolster its allegations by relying primarily on two cases to show that Wells Fargo breached an independent duty of care. Opposition Brief at 24-30. Both are distinguishable. First, while Wells Fargo did owe a duty of care to BDA as its customer, this duty arose out of, and was limited to, the contractual relationship between the parties. Opening Brief at 24-25. In response, BDA cites *Chaney v. Dreyfus Service Corp.*, 595 F.3d 219 (5th Cir. 2010), a Fifth Circuit decision examining the duty of an investment broker to safeguard the insurance funds of its clients.[9] Opposition Brief at 25-26. However, the duty of care at issue in *Chaney* was "to ensure that an individual purporting to trade on [a] customer's behalf is actually authorized to do so." *Chaney*, 595 F.3d at 235. This is distinct from Wells Fargo's duty to process verified payment orders received from BDA, which arose out of and was specifically defined by the Agreement. *See supra* Section I.B.

Second, even accepting BDA's contention that Wells Fargo owed it an independent duty, its formulation of that duty – one that requires a bank to recognize, stop in real-time, and inquire about "suspicious or extraordinary transactions" – is inapplicable. Opposition Brief at 28-29. There was nothing "unusual or anomalous," let alone "suspicious or extraordinary," about the

[9] The other case BDA cites did not reach whether an independent duty of care was owed to plaintiff. *See Dubai Islamic Bank v. Citibank, N.A.*, 126 F. Supp. 2d 659, 667 (S.D.N.Y. 2000).

payment orders Wells Fargo received. *See supra* Section I.C, Opening Brief at 14. Plaintiff appears to have based its newfound "suspicious or extraordinary" standard on *Chaney*, where the Fifth Circuit held that employees of the defendant broker should have recognized the relevant transactions "as suspicious and extraordinary, particularly with respect to the funds of an insurance company." *Chaney*, 595 F.3d at 236. But *Chaney*, where defendant broker "took no steps to verify" that the transactions were authorized beyond accepting the "unverified word" of its clients' purported representative, *id.* at 235-36, is far different from the facts here, where BDA admits that Wells Fargo verified the payment orders pursuant to the Agreement.[10]

BDA's reliance on *Dubai Islamic Bank* is similarly misplaced. There, plaintiff alleged that the defendant failed to comply with its KYC policies because it permitted a "reputed international financial terrorist" to open an account that was then used, with the aid of bank employees, to inappropriately debit plaintiff's correspondent account. *Dubai Islamic Bank*, 126 F. Supp. 2d at 662-63. The duty at issue in *Dubai Islamic Bank* is distinct from Wells Fargo's duty to verify payment orders. As explained, KYC policies and related statutes are designed specifically to prevent the harm that the defendant in *Dubai Islamic Bank* permitted, but Wells Fargo's compliance with such policies is not at issue. *See supra* Section I.B. There are no allegations that Wells Fargo failed to conduct due diligence prior to accepting a customer who then stole BDA's funds, and AML and KYC policies do not create a duty to monitor customer accounts and question validly authorized payment orders for the benefit of the customer. *See* Opening Brief at 25-26. To impose such a duty would not only be inconsistent with, and render

---

[10] BDA correctly states that the Second Circuit has held that a bank has a duty to make reasonable inquires to prevent fraud when it has notice or knowledge of such fraud. *See 2006 Frank Calandra, Jr. Irrevocable Tr. v. Signature Bank Corp.*, 503 F. App'x 51, 54 (2d Cir. 2012); Opposition Brief at 28. However, the Second Circuit also explained that such notice, and the related duty, does not exist where, as here, the defendant "had every reason to believe that the transactions were valid and authorized." *Signature Bank*, 503 F. App'x at 54.

meaningless, the N.Y. U.C.C., *see infra* Section III, but it would also require receiving banks to undertake the nearly impossible task of determining which facially valid payment orders are actually authorized, a task for which plaintiffs are far better suited. *See* Opening Brief at 26.

III. BDA's Common Law Claims Are Inconsistent With the N.Y. U.C.C.[11]

The parties agree that the N.Y. U.C.C. preludes common law claims that are inconsistent with Article 4-A, and New York courts have held that claims involving allegations of fraudulent and unauthorized wire transfers and noncompliance with security procedures are precluded. *See, e.g.*, *Centre-Point Merch. Bank Ltd. v. Am. Express Bank Ltd.*, 913 F. Supp. 202, 208 (S.D.N.Y. 1996) (ruling that claims regarding the "payment of fraudulent payment orders, allegedly in breach of a duty to provide commercially reasonable security" were precluded by Article 4-A). BDA's attempt to remove its claims from these precedents by refashioning them as allegations that Wells Fargo "should have known . . . that the funds were fraudulently obtained," Opposition Brief at 31, 33-34, is not only inconsistent with the Complaint, but also fails as a matter of law. *See* Opening Brief at 18-22. The Complaint is silent about Wells Fargo's knowledge that the payment orders were actually fraudulent, stating only that Wells Fargo should have been alerted to the allegedly suspicious nature of the transactions. Compl. ¶¶ 73-75. BDA cannot now recast its claims simply because it belatedly realized that they are prohibited by the N.Y. U.C.C.

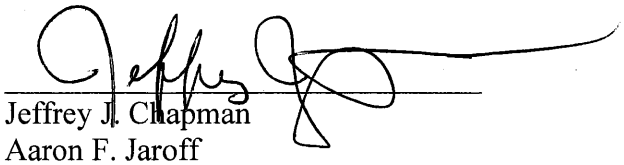
CONCLUSION

For the foregoing reasons, and for those stated in its Opening Brief, Wells Fargo respectfully requests that the Complaint be dismissed in its entirety, with prejudice.

---

[11] BDA argues that it has stated a breach of contract claim because Wells Fargo allegedly failed to comply with the Agreement's additional statutory "restrictions." Opposition Brief at 22 n.17. This argument fails because such terms were not part of the Agreement and Wells Fargo complied with the security procedure. *See supra* Section I.B; Opening Brief at 26-29.

Dated: New York, New York
April 25, 2016

By: 

Jeffrey J. Chapman
Aaron F. Jaroff
McGuireWoods LLP
1345 Avenue of the Americas, 7th Floor
New York, New York 10105-0106
(212) 548-2100
jchapman@mcguirewoods.com
ajaroff@mcguirewoods.com

Attorneys for Defendant Wells Fargo Bank, N.A.